PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-216897
(43)Date of publication of application : 05.08.1994

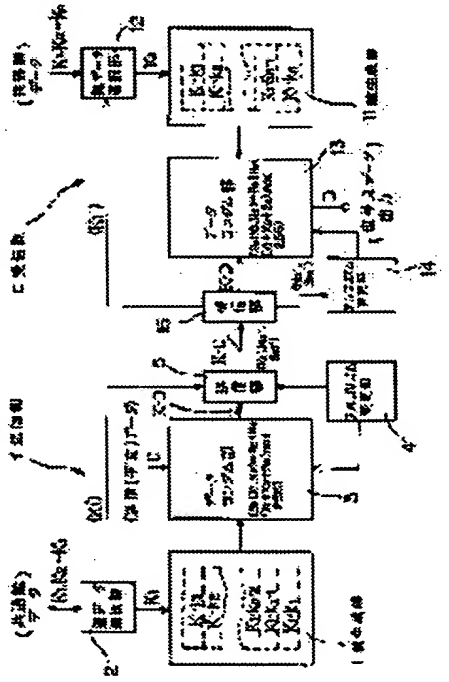
(51)Int.CI. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 05-024750
(22)Date of filing : 20.01.1993

(71)Applicant : NIPPON SIGNAL CO LTD:THE
(72)Inventor : AOYANAGI HIDEYUKI

(54) DATA TRANSMITTER-RECEIVER

(57)Abstract:
PURPOSE: To allow the transmitter-receiver to cope with a fact that the strength of ciphering is high and a common key might be decoded by storing plural common key data in advance and revising the common key under a prescribed condition.
CONSTITUTION: A sender side is provided with a key generating section 1 generating plural kinds of sub keys based on a prescribed common key K1. The common key K1 fed to the key generating section 1 is selected alternatively by a key data selection section 2 from plural common keys K1-Kn stored in advance in a memory of a transmission side and a data random section 3 uses sub keys K1.K1-K1.Kn of the key generating section 1 to generate a ciphered sentence K/D according to a prescribed algorithm from transmission data D. A key data generating section 11 on a receiver side generates plural kinds of sub keys K1.K1-K1.Kn based on the common key K1 and a data random section 13 decodes the ciphered sentence K.D received from a reception section 15 according to a prescribed algorithm. The key data selection section 2 on the sender side selects a common key under a certain condition such as that after lapse of prescribed time.



LEGAL STATUS

[Date of request for examination]	24.12.1999
[Date of sending the examiner's decision of rejection]	28.01.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's	

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－216897

(43)公開日　平成6年(1994)8月5日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		8837－5L			
			7117－5K	Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数３　ＦＤ　（全　５　頁）

(21)出願番号　特願平5－24750

(22)出願日　平成５年(1993)１月20日

(71)出願人　000004651
日本信号株式会社
東京都千代田区丸の内３丁目３番１号

(72)発明者　青柳　秀幸
埼玉県浦和市上木崎１丁目13番８号　日本信号株式会社与野事業所内

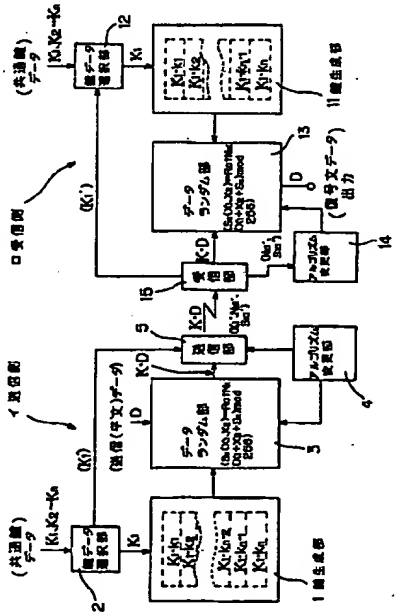
(74)代理人　弁理士　石井　光正

(54)【発明の名称】　データ送受信装置

(57)【要約】

【目的】　共通鍵が解読されたとしても、すぐに別の共通鍵に変更できるとともに、データランダム部のアルゴリズムも変更可能にして、極めて暗号強度の高いデータ送受信装置を得る。

【構成】　送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置であって、複数の共通鍵データを予め格納する鍵データ格納手段と、所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段とを有している。



1

【特許請求の範囲】

【請求項１】　送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、
複数の共通鍵データを予め格納する鍵データ格納手段と、
所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、
を設けたことを特徴とするデータ送受信装置。

【請求項２】　送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、
前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段を設けたことを特徴とするデータ送受信装置。

【請求項３】　送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、
複数の共通鍵データを予め格納する鍵データ格納手段と、
所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、
前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段と、
を設けたことを特徴とするデータ送受信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データ送受信装置に係り、特に暗号強度が高く、例えば、通信機能を備えたＩＣカード型の非接触式定期券を用いる自動改札システムに好適なものに関する。

【０００２】

【従来の技術】従来、交信するデータの秘密を保持するために、データ内容を暗号化して通信を行うことが行わ

2

れている。この場合、通常、共通鍵暗号通信方式が採用されている。

【０００３】共通鍵暗号通信方式は、受信相手Ａに送信すべきデータ（以下、平文データというときもある）Ｄがあるとき、先ず、受信相手Ａと共通の共通鍵データ（以下、共通鍵という）K_C を用いて暗号文K_C・Ｄを作り、この暗号文K_C・Ｄを受信相手Ａに送信し、他方、暗号文K_C・Ｄを受信した受信相手Ａは、暗号文K_C・Ｄを共通鍵K_C を用いて復号処理してデータＤを抽出するようにしている。

【０００４】この共通鍵方式のデータ送受信装置においては、通常、鍵生成部において共通鍵K_C を基にサブ鍵を多種生成するとともに、その生成されたサブ鍵を用いてデータランダム部で所定のアルゴリズムに従って平文データＤを暗号化したり、又は復号化するようにしている。

【０００５】ところで、非接触式定期券は、磁気カード式の定期券に比べ、記憶容量が大きいので、定期券の機能の他に、例えば駅の売店等で買物もできるようなストアード・フェアカードとしての機能も持たせることが考えられる。このような多機能型とすると、非接触式定期券はもはや単なる定期券ではなくなり、一種の金券の性格を有するので、データの改ざんを困難にして安全性を確保することが望まれている。このため、自動改札機と非接触式定期券との間で交信されるデータを暗号化することが考えられている。

【０００６】

【発明が解決しようとする課題】しかしながら、共通鍵データを用いて暗号文化してデータ授受を行うデータ送受信装置においては、一旦、共通鍵が解読されてしまうと、データの改ざんを許してしまうこととなる。

【０００７】このような不正を阻止する手段としては、共通鍵のビット数を多くして、解読を困難にし、暗号強度を高めることも考えられる。

【０００８】しかし、単にビット数を多くしても、共通鍵が解読されたときは、データ送受信装置のシステムを変更しなければならない。

【０００９】殊に、非接触式自動改札システムにおいて、共通鍵が解読されたときは、システム変更の対象となる機器類が膨大であるため、大変な費用を必要とする。

【００１０】そこで、本発明は、上記問題点を解決するためになされたものであって、その目的は、暗号強度が高く、仮りに共通鍵が解読されたとしても、速やかに対応できるデータ送受信装置を提供することにある。

【００１１】

【課題を解決するための手段】本発明に係るデータ送受信装置は、送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に

送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、複数の共通鍵データを予め格納する鍵データ格納手段と、所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段とを設けたことを特徴としている。また、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段を設けたことを特徴としている。さらに、複数の共通鍵データを予め格納する鍵データ格納手段と、所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段とを設けたことを特徴としている。

【００１２】

【作用】上記構成において、鍵データ選択手段は、所定の条件下で共通鍵データを変更する。したがって、それまでの共通鍵は無効となり、それまで使用されていた共通鍵が解読されても支障が生じない。また、アルゴリズム変更手段は、所定の条件下で平文データを暗号化するアルゴリズムを変更する。したがって、仮に共通鍵が解読され、かつ暗号文が復号化できたとしても、アルゴリズム変更後は、暗号文の復号化が困難となる。さらに鍵データ選択手段とアルゴリズム変更手段とを備えると、暗号強度は格段に向上する。

【００１３】

【実施例】以下、本発明の実施例を図面に基づいて説明する。図１は、一実施例装置の概略構成を示すブロック図であって、送信側イには、所定の共通鍵（図示の例ではK_1）を基に複数種のサブ鍵$K_1 \cdot k_1 \sim K_1 \cdot k_n$を生成する鍵生成部１が設けられている。

【００１４】鍵生成部１に供給される共通鍵K_1は、送信側イに設けられている図示しないメモリに予め格納されている複数の共通鍵$K_1 \sim K_n$から、鍵データ選択部２により択一的に選択されるように構成されている。

【００１５】データランブム部３は、鍵生成部１のサブ鍵$K_1 \cdot k_1 \sim K_1 \cdot k_n$を用いて、平文データＤを所定のアルゴリズムに従って暗号文Ｋ・Ｄを生成するように構成されている。

【００１６】このアルゴリズムは、共通鍵暗号方式として一般的に用いられているフェイル（Ｆｅａｌ）－８方式のｆ関数のＳ－ボックス（ＢＯＸ）が格納されている。周知のＳ－ＢＯＸは、$S_1(X_1, X_2) = Rot2(X_1 \times X_2 + S_1) \bmod 256$であるが、本実施例のＳ－ＢＯＸは、式中の「２」及び「S_1」がアルゴリズム変更部４によって変更されるように、つまり、$S \times (X_1, X_2) = RotN_x (X_1 + X_2 + S_x) \bmod 256$に構成されている。

【００１７】送信部５は、周知の増幅器を備えて構成され、データランダム部３からの暗号文Ｋ・Ｄを受信側Ｄへ送信できるように構成されているとともに、受信側イで使用中の共通鍵（図示の例ではK_j）の選択データ（K_1'）と、使用中のアルゴリズムの変数識別データ（N_x'，S_x'）とを受信側ロへ送出するように構成されている。

【００１８】受信側ロには、送信側イと同一構成の鍵生成部１１，鍵データ選択部１２，データランダム部１３及びアルゴリズム変更部１４を備えているとともに、送信側イの送信部５に対応した受信部１５を備えている。また、送信側イの図示しないメモリには、送信側イと同様に複数の共通鍵K_1，$K_2 \cdots K_n$が予め格納されている。

【００１９】次に、本実施例装置の動作について説明する。今、鍵データ選択部２は、共通鍵K_1を選択し、かつアルゴリズム変更部４はＳ－ＢＯＸの変数をN_{x1}，S_{x1}を選択しているものとする。したがって、送信部５からは使用中の共通鍵とアルゴリズムを識別するための信号（K_1'，N_{x1}'，S_{x1}'）が受信側ロに送出される。

【００２０】鍵生成部１では、選択された共通鍵K_1を用いて複数種（Ｆｅａｌ－８の場合は８個）のサブ鍵$K_1 \cdot k_1 \sim K_1 \cdot k_n$を生成し、データランダム部３では、これらサブ鍵$K_1 \cdot k_1 \sim K_1 \cdot k_n$を用いて変数$N_{x1}$，$S_{x1}$のアルゴリズムに従って平文データＤを暗号文Ｋ・Ｄに変換する。そして、この暗号文Ｋ・Ｄは、送信部５から受信側ロへ送出される。

【００２１】受信部５は、受信信号から使用中の共通鍵データ（K_1'）と使用中アルゴリズムの識別データ（N_{x1}'，S_{x1}'）を鍵データ選択部１２及びアルゴリズム変更部１４にそれぞれ送出する。したがって、鍵データ選択部１２は、共通鍵K_1を選択するとともに、データランダム部１３は変数N_{x1}，S_{x1}を選択する。

【００２２】鍵データ生成部１１は、共通鍵K1 に基づいて複数種のサブ鍵K1 ・k1 ～K1 ・kn を生成するとともに、データランダム部１３は、受信部１５から入力した暗号文Ｋ・Ｄを変数Nx1，Sx1の所定のアルゴリズムに従って復号処理して復号文Ｄを抽出する。

【００２３】送信側イの鍵データ選択部２及びアルゴリズム変更部４は、一定の条件下で、例えば所定時間経過後に、あるいは、当日の天候の状態による等の全く不規則的に共通鍵を選択し、さらにアルゴリズムを変更するようにしてある。

【００２４】したがって、第三者が故意に一時的に使用されている共通鍵及びアルゴリズムを膨大な時間と費用を費やして解読したときには、既に、別の共通鍵とアルゴリズムが使用されているので、その解読は全く意味をなさないこととなる。このため、極めて暗号強度の高い

5

データ送受信装置とすることができる。

【００２５】なお、上述の実施例では、共通鍵とアルゴリズムを同時に変更するようにしたが、どちらか一方だけでもよく、又は両者を交互に変更するようにしてもよい。

【００２６】

【発明の効果】本発明に係るデータ送受信装置は、共通鍵又はデータランダム部のアルゴリズムを所定の条件下で変更するようにしたので、極めて暗号強度が高く、仮に共通鍵が解読されても、すぐに他の共通鍵に変更することが可能である。また、共通鍵とアルゴリズムの両方を変更するようにすると、より暗号強度を高めることが可能となる。

6

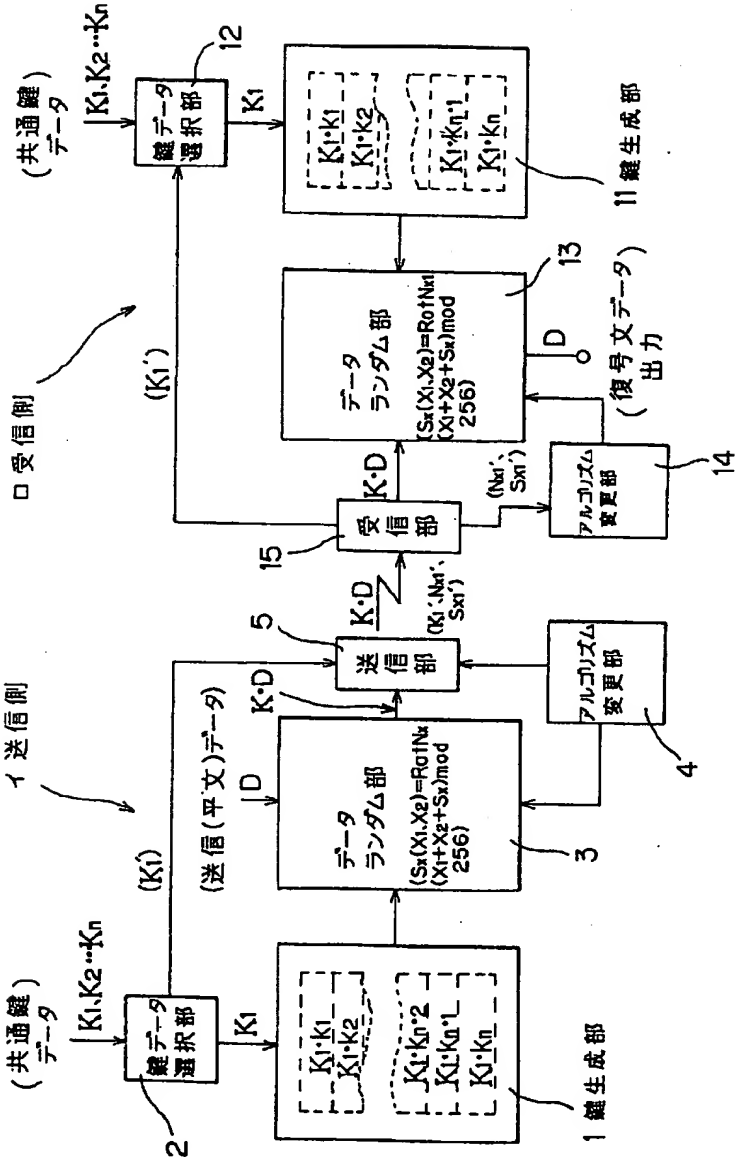
【図面の簡単な説明】

【図１】本発明の一実施例装置の概略構成を示すブロック図である。

【符号の説明】

１，１１	鍵生成部
２，１２	鍵データ選択部（鍵データ選択手段）
３，１３	データランダム部
４，１４	アルゴリズム変更部（アルゴリズム変更手段）
５	送信部
１５	受信部
イ	送信側
ロ	受信側

【図1】


イ 送信側
ロ 受信側
(共通鍵)データ
K1,K2…Kn
鍵データ選択部
K1
K1'
(K1')
(送信(平文)データ)
D
K·D
データランダム部
(Sx(X1,X2)=RotNx1(X1+X2+Sx)mod 256)
アルゴリズム変更部
送信部
受信部
(Nx1', Sx1')
(K1', Nx1', Sx1')
(復号文データ)出力
1 鍵生成部
2
3
4
5
11 鍵生成部
12
13
14
15

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.